

Обзор
Директивы ОЭСР по проблеме
безопасности информационных систем и
сетей: формирование культуры
обеспечения безопасности

Overview

OECD Guidelines for the Security of Information Systems
and Networks: Towards a Culture of Security

Russian translation

Обзоры – это переводы выдержек из публикаций ОЭСР.
Их можно получить бесплатно в онлайн-магазине ОЭСР

www.oecd.org/bookshop/

Данный обзор не является официальным переводом ОЭСР.



ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT

ОРГАНИЗАЦИЯ ЭКОНОМИЧЕСКОГО СОТРУДНИЧЕСТВА И РАЗВИТИЯ

Директивы по проблеме безопасности информационных систем и сетей: формирование культуры обеспечения безопасности

ПРЕДИСЛОВИЕ

За период, прошедший с 1992 г., когда ОЭСР впервые представила “Директивы по проблеме безопасности информационных систем”, в сфере применения информационных систем и сетей, равно как и информационных технологий в целом, произошли коренные изменения. Эти перемены, продолжающиеся и по сей день, принесли существенную выгоду, однако при этом они потребовали и гораздо более серьезного внимания к сфере безопасности со стороны правительств, коммерческих предприятий, иных организаций и частных пользователей, которые разрабатывают информационные системы и сети, владеют ими, предоставляют их в пользование, управляют ими, обслуживают или используют их (“участвующие стороны”).

На смену довольно скромным по возможностям автономным системам, работавшим, как правило, в изолированных сетях, пришли гораздо более высокопроизводительные персональные компьютеры, разработки на стыке различных научных направлений, повсеместное распространение получил Интернет. Сегодня участвующие стороны становятся все в большей мере связанными друг с другом, причем связи эти пересекают границы государств. Кроме того, Интернет обеспечивает функционирование столь важных компонентов инфраструктуры, как энергетика, транспорт и финансовый сектор, и в очень существенной степени определяет то, каким образом компании ведут свой бизнес, как правительства и органы государственного управления предоставляют услуги гражданам и предприятиям и как граждане общаются между собой и обмениваются информацией друг с другом. Характер и тип технологий, образующих информационную инфраструктуру и инфраструктуру связи, также существенным образом изменились. Количество и многообразие устройств для доступа к этим видам инфраструктуры возросли многократно, и теперь в их состав входят фиксированные, беспроводные и мобильные устройства, причем постоянно увеличивается процент устройств, доступ через которые осуществляется в непрерывном режиме через постоянно работающие каналы связи. Как следствие всего этого, значительно выросли разнообразие, объем и степень секретности пересылаемой информации.

Как следствие увеличения числа связей и объемов обмена данными между информационными системами и сетями, эти системы и сети подвергаются сейчас растущему количеству и более широкому разнообразию угроз и факторов риска. В связи с этим, в сфере обеспечения безопасности возникают новые проблемы. По этим причинам настоящие Директивы распространяются на все участвующие стороны информационного общества и дают основания полагать, что существует необходимость расширения осведомленности о существовании проблем в сфере обеспечения безопасности и достижения лучшего понимания сути этих проблем, а также необходимость формирования так называемой “культуры обеспечения безопасности”.

I. ФОРМИРОВАНИЕ КУЛЬТУРЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Настоящие Директивы призваны помочь справиться с проблемами, возникающими в постоянно меняющейся сфере безопасности, путем поощрения формирования культуры обеспечения безопасности. Иными словами, упор делается на необходимость обеспечения безопасности при разработке информационных систем и сетей и принятие новой модели мышления и поведения при использовании информационных систем и сетей и при взаимодействии с ними. Принятие данных Директив знаменует собой принципиальную перемену в самом отношении к обеспечению защищенной структуры и безопасной эксплуатации сетей и систем по сравнению с тем, что было раньше (в прошлом, очень во многих случаях проблемы безопасности пытались решать “задним числом”, т.е. тогда, когда было уже слишком поздно). Участвующие стороны все в большей мере зависят от информационных систем, сетей и связанных с ними услуг, и все эти системы, сети и услуги должны стать более надежными и защищенными. Безопасность может быть надежно обеспечена только при принятии такого подхода, при котором в надлежащей мере учитываются интересы всех участвующих сторон и основные свойства систем, сетей и связанных с ними услуг.

Деятельность каждой из участвующих сторон имеет важное обеспечение для обеспечения безопасности. Участвующие стороны, в соответствии со своими ролями и функциями, должны быть осведомлены о соответствующих рисках в сфере безопасности и превентивных мерах, они должны брать на себя ответственность и принимать меры, направленные на повышение безопасности информационных систем и сетей.

Для того, чтобы стимулировать формирование и совершенствование культуры обеспечения безопасности, потребуются как руководство, так и широкое участие заинтересованных сторон, и это должно привести к повышению приоритетности вопросов планирования и руководства обеспечением безопасности, а также к осознанию всеми участвующими сторонами необходимости обеспечения безопасности. Проблемами обеспечения безопасности должны заниматься на всех уровнях государственного управления и коммерческих предприятий, равно как и все участвующие стороны. Настоящие Директивы образуют основу, на которой должна строиться работа по формированию в обществе культуры обеспечения безопасности.

Это позволит участвующим сторонам учитывать фактор безопасности при проектировании и эксплуатации всех информационных систем и сетей. В Директивах предлагается, чтобы все участвующие стороны сформировали у себя и развивали культуру обеспечения безопасности как способ мышления, оценки и принятия мер, касающихся функционирования информационных систем и сетей.

II. ЦЕЛИ И ЗАДАЧИ

Цели и задачи настоящих Директив таковы:

- способствовать совершенствованию у всех участвующих сторон культуры обеспечения безопасности как средства защиты информационных систем и сетей;
- повысить осведомленность о факторах риска для информационных систем и сетей, о существующих политике, практике, мерах и процедурах, направленных на защиту от этих рисков, и о необходимости принятия и реализации этих политики, практики, мер и процедур;
- поощрять формирование у всех участвующих сторон большего доверия к информационным системам и сетям и к тому способу, которым они предоставляются в пользование и используются;
- создать общую концептуальную основу, которая поможет участвующим сторонам понять суть проблем в сфере безопасности и отнестись со вниманием к этическим ценностям при выработке и реализации логически последовательных политики, практики, мер и процедур обеспечения безопасности информационных систем и сетей;
- способствовать сотрудничеству и обмену информацией, насколько это будет уместным, между всеми участвующими сторонами при выработке и реализации политики, практики, мер и процедур в области безопасности;
- содействовать тому, чтобы все участвующие стороны, вовлеченные в разработку и реализацию стандартов и норм, признавали важность задачи обеспечения безопасности.

III. ОСНОВНЫЕ ПРИНЦИПЫ

Нижеприведенные девять принципов являются взаимодополняющими, и их следует рассматривать как единое целое. Они относятся к участвующим сторонам на всех уровнях, включая политический и оперативный. Согласно настоящим Директивам, обязанности участвующих сторон будут зависеть от выполняемых ими функций и ролей. Все участвующие стороны только выиграют от улучшения своей информированности, им пойдет на пользу привитие соответствующих навыков, совместное использование информации и обучение, а это позволит им глубже понять суть проблем безопасности и совершенствовать практические действия в этой сфере. Меры и усилия по повышению безопасности информационных систем и сетей не

должны противоречить ценностям демократического общества и, в частности, необходимости существования свободных и открытых информационных потоков и такому основополагающему тезису, как необходимость обеспечения неприкосновенности частной жизни.¹

1) Осведомленность

Участвующие стороны должны осознавать необходимость обеспечения безопасности информационных систем и сетей и понимать, что они могут сделать для повышения безопасности.

Осведомленность о факторах риска и существующих мерах безопасности можно рассматривать как первый “рубеж обороны” при обеспечении безопасности информационных систем и сетей. На информационные системы и сети могут воздействовать как внутренние, так и внешние риски. Участвующие стороны должны отдавать себе отчет в том, что сбои в системе безопасности могут привести к нанесению существенного ущерба системам и сетям, находящимся под их контролем. Они также должны быть осведомлены о том возможном ущербе, который может быть нанесен другим вследствие взаимного подключения и взаимной зависимости между системами и сетями. Участвующие стороны должны знать конфигурацию своей системы, и в их распоряжении должна быть информация о существующих обновлениях к ней, о месте системы в сетях, о надлежащих приемах работы, которые они могут внедрить для повышения безопасности, а также о нуждах и потребностях других участвующих сторон.

2) Ответственность

За безопасность информационных систем и сетей отвечают все участвующие стороны.

Взаимосвязанные локальные и глобальные информационные системы и сети играют важную роль в обеспечении нормальной работы участвующие стороны, и эти стороны должны осознавать свою ответственность за обеспечение безопасности этих информационных систем и сетей. Они должны отвечать за свои действия в соответствии с выполняемыми ими функциями и ролями. Участвующие стороны должны регулярно анализировать свои собственные политику, практику, меры и процедуры и оценивать, насколько они соответствуют сложившейся у них ситуации. Те, кто разрабатывает, проектирует и поставяет продукты и услуги, должны в процессе своей работы уделять внимание вопросам обеспечения безопасности систем и сетей и своевременно рассылать соответствующую информацию, включая обновления, с тем, чтобы пользователи смогли лучше понять функциональные возможности продуктов и услуг, относящиеся к обеспечению безопасности, и свои обязанности по обеспечению безопасности.

¹ Помимо данных Директив по проблеме безопасности, ОЭСР подготовила дополняющие их рекомендации, содержащие руководящие указания по другим вопросам, имеющим важное значение для всемирного информационного общества. Они касаются неприкосновенности частной жизни (“Директивы ОЭСР, регламентирующие обеспечение неприкосновенности частной жизни и защиту трансграничных потоков данных о частных лицах”, принятые в 1980 г.) и криптографии (“Директивы, регламентирующие политику в сфере криптографии”, принятые в 1997 г.). Настоящие Директивы по проблеме безопасности должны истолковываться в едином комплексе с означенными документами.

3) *Принятие ответных мер*

Участвующие стороны должны, в сотрудничестве с другими, предпринимать своевременные действия для предотвращения, выявления и реагирования на инциденты, связанные с нарушениями безопасности.

Осознавая взаимосвязь и взаимозависимость информационных систем и сетей и потенциальную возможность того, что этим системам, в принципе, могут быть в течение короткого времени нанесены масштабные повреждения, участвующие стороны должны своевременно, проявляя готовность к сотрудничеству друг с другом, реагировать на инциденты, связанные с нарушениями безопасности. Они должны делиться друг с другом – в зависимости от конкретной ситуации – сведениями об угрозах и уязвимых местах, а также реализовывать процедуры, предусматривающие быстрое и действенное налаживание сотрудничества для предотвращения и выявления инцидентов, связанных с нарушением безопасности, и реагирования на них. В тех случаях, когда это будет допустимым, могут предусматриваться трансграничное совместное использование информации и международное сотрудничество.

4) *Этика*

Участвующие стороны должны учитывать законные интересы других лиц и организаций.

Учитывая широкое распространение информационных систем и сетей в нашем обществе, участвующие стороны должны осознать, что их действие или бездействие может нанести ущерб другим лицам и организациям. Поэтому крайне важно этическое поведение, и участвующие стороны должны приложить усилия для выработки и внедрения наиболее оптимальных методов работы и стимулирования такого поведения, при котором осознается необходимость обеспечения безопасности и уважаются законные интересы других.

5) *Демократия*

Обеспечение безопасности информационных систем и сетей не должно вступать в противоречие с основополагающими ценностями демократического общества.

Безопасность должна реализовываться таким образом, чтобы это сочеталось с ценностями, признаваемыми в демократическом обществе, такими, в частности, как свобода обмена мнениями и идеями, свободный обмен информацией, конфиденциальность информации и связи, надлежащая защита личной информации, открытость и информационная прозрачность.

6) *Оценка рисков*

Участвующие стороны должны проводить оценку рисков.

В ходе оценки рисков выявляются угрозы и уязвимые места, причем такая оценка должна быть в достаточной степени всеобъемлющей, чтобы учесть важнейшие внутренние и внешние факторы, к числу которых относятся технологические, физические и человеческие факторы, политика и услуги третьих сторон, оказывающие влияние на обеспечение безопасности. Оценка рисков позволит определить приемлемый

уровень риска и помочь в выборе надлежащих средств и методов управления в ситуации, когда существует риск нанесения ущерба информационным системам и сетям, при этом должны приниматься во внимание характер и важность защищаемой информации. Ввиду растущей взаимосвязи и взаимозависимости между информационными системами, оценка рисков должна включать в себя анализ потенциального ущерба, который может исходить от других лиц и организаций или может быть нанесен им.

7) Разработка и реализация систем и сетей с учетом необходимости обеспечения безопасности

Участвующие стороны должны рассматривать безопасность как один из наиболее важных элементов информационных систем и сетей.

Для обеспечения оптимального уровня безопасности необходимы надлежащие разработка, реализация и координирование систем, сетей и политики. Главным, но не единственным направлением этой деятельности является разработка и внедрение надлежащих мер безопасности и решений, призванных устранить или ограничить потенциальный ущерб, обусловленный существованием выявленных угроз и уязвимых мест. Для этого требуются меры безопасности и решения как технического, так и нетехнического характера, и они должны быть соразмерны ценности информации, хранимой в системах и сетях соответствующей организации. Обеспечение безопасности должно быть основополагающим свойством всех продуктов, услуг, систем и сетей, равно как и неотъемлемой составной частью проектов и архитектуры систем. Для конечных пользователей проектирование и реализация с учетом фактора безопасности в значительной мере сводится к выбору и конфигурированию продуктов и услуг для своей системы.

8) Руководство обеспечением безопасности

Участвующие стороны должны принять комплексный подход к руководству обеспечением безопасности.

Руководство обеспечением безопасности должно основываться на оценке рисков. Оно должно быть динамичным, охватывающим все уровни деятельности участвующих сторон и все аспекты их работы. Оно должно включать в себя упреждающее реагирование на появляющиеся угрозы и должно предусматривать принятие мер, направленных на предотвращение и выявление инцидентов и реагирование на них, мер по восстановлению систем после сбоев, непрерывное техническое обслуживание, анализ и аудит. Политика, практика, меры и процедуры в области обеспечения безопасности информационных систем и сетей должны быть скоординированными и интегрированными с тем, чтобы образовывать логически последовательную систему обеспечения безопасности. Требования к руководству обеспечением безопасности зависят от уровня участия, роли и функций участвующей стороны, существующего риска и требований к системе.

9) Повторная оценка

Участвующие стороны должны анализировать и проводить повторную оценку безопасности информационных систем и сетей, а также вносить соответствующие изменения в политику, практику, меры и процедуры в сфере безопасности.

Постоянно выявляются новые, постоянно меняющиеся угрожающие факторы и уязвимые места. Участвующие стороны должны непрерывно анализировать, повторно оценивать и вносить изменения во все элементы комплекса мер по обеспечению безопасности, чтобы противостоять этим меняющимся факторам риска.

Рекомендация Совета по поводу Директив по проблеме безопасности информационных систем и сетей: формирование культуры обеспечения безопасности

СОВЕТ,

принимая во внимание Конвенцию о создании Организации экономического сотрудничества и развития от 14 декабря 1960 г. и, в частности, статьи 1 b), 1 c) и 5 b) указанного документа,

принимая во внимание Рекомендацию Совета по поводу Директив, регламентирующих обеспечение неприкосновенности частной жизни и защиту трансграничных потоков данных о частных лицах, от 23 сентября 1980 г. [C(80)58(Final)],

принимая во внимание Декларацию о трансграничных потоках данных, принятую Правительствами стран-членов ОЭСР 11 апреля 1985 г. [Приложение к документу C(85)139],

принимая во внимание Рекомендацию Совета по поводу Директив, регламентирующих политику в сфере криптографии, от 27 марта 1997 г. [C(97)62/FINAL],

Принимая во внимание Декларацию об обеспечении неприкосновенности частной жизни в глобальных сетях, принятую на уровне министров 7-9 декабря 1998 г. [Приложение к документу C(98)177/FINAL],

принимая во внимание Декларацию об аутентификации в электронной коммерции, принятую на уровне министров 7-9 декабря 1998 г. [Приложение к документу C(98)177/FINAL],

признавая, что информационные системы и сети используются правительствами, коммерческими предприятиями, иными организациями и частными пользователями во все более широких масштабах и что важность и значимость этих систем и сетей постоянно возрастает,

признавая, что постоянно растущая значимость и роль информационных систем и сетей, а также растущая зависимость от них в деле обеспечения стабильного и эффективного функционирования национальной экономики различных государств и международной торговли, а также в социальной, культурной и политической жизни требуют принятия особых мер по защите таких систем и сетей и по укреплению доверия к ним,

признавая, что внедрение информационных систем и сетей и их распространение по всему миру связаны с появлением новых и возрастающих факторов риска,

признавая, что существует угроза безопасности данных и информации, хранимых в информационных системах и сетях или передаваемых по ним, обусловленная возможностью разного рода несанкционированного доступа, использования, неправомерного присвоения, изменения, пересылки вредоносных программ, отказа в обслуживании или уничтожения вышеупомянутых данных и информации, и что требуются надлежащие меры защиты,

признавая, что существует необходимость повысить осведомленность о факторах риска для информационных систем и сетей и о существующих политике, практике, мерах и процедурах, направленных на противодействие этим факторам риска, а также необходимость поощрения надлежащего поведения как важнейший шаг, направленный на формирование культуры обеспечения безопасности,

признавая, что необходим пересмотр существующих политики, практики, мер и процедур, чтобы они позволяли успешно решать меняющиеся задачи и проблемы, возникающие в связи с угрозами безопасности информационных систем и сетей,

признавая, что существует общая заинтересованность в обеспечении безопасности информационных систем и сетей путем формирования культуры обеспечения безопасности, причем эта заинтересованность благоприятствует координации действий и сотрудничеству в международных масштабах, с тем, чтобы успешно решать проблемы, возникающие в связи с тем ущербом, который может быть нанесен экономике различных государств, международной торговле и участию граждан в социальной, культурной и политической жизни из-за сбоев в системе безопасности,

а также признавая, что *“Директивы по проблеме безопасности информационных систем и сетей: формирование культуры обеспечения безопасности”*, приведенные в Приложении к данной Рекомендации, подлежат исполнению на добровольной основе и не затрагивают суверенных прав государств,

и признавая, что эти Директивы не являются основанием для предположений о том, для обеспечения безопасности существует какое-либо одно конкретное решение, и о том, какие именно политика, практика, меры и процедуры пригодны для какой-либо конкретной ситуации; напротив, в данных Директивах изложена совокупность принципов, призванных содействовать формированию более четкого представления о том, как участвующие стороны могут извлечь для себя выгоду от развития и совершенствования культуры безопасности и внести свой вклад в ее развитие и совершенствование,

РЕКОМЕНДУЕТ ДЛЯ ПРИМЕНЕНИЯ настоящий документ, озаглавленный *“Директивы по проблеме безопасности информационных систем и сетей: формирование культуры обеспечения безопасности”*, правительствам, коммерческим предприятиям, иным организациям и частным пользователям, которые разрабатывают информационные системы и сети, владеют ими, предоставляют их в пользование, управляют ими, обслуживают или используют их,

РЕКОМЕНДУЕТ странам-членам ОЭСР:

принять новые или внести изменения в действующие политику, практику, меры и процедуры с тем, чтобы учесть и отразить в них *“Директивы по проблеме безопасности*

информационных систем и сетей: формирование культуры обеспечения безопасности” посредством восприятия и поощрения развития культуры обеспечения безопасности в соответствии с Директивами,

проводить консультации, координировать свои действия и осуществлять сотрудничество на национальном и международном уровне с целью реализации данных Директив,

распространять данные Директивы в государственном и частном секторах, в том числе, среди правительств, коммерческих предприятий, иных организаций и частных пользователей с тем, чтобы содействовать формированию и укреплению культуры обеспечения безопасности и поддержать все заинтересованные стороны в их стремлении проявлять ответственное отношение к данной проблеме и принимать необходимые меры для реализации указанных Директив таким образом, чтобы это соответствовало выполняемым этими правительствами, предприятиями, организациями и частными лицами функциям,

своевременно и надлежащим образом предоставить данные Директивы в распоряжение стран, не являющихся членами ОЭСР,

пересматривать Директивы каждые пять лет с тем, чтобы способствовать развитию международного сотрудничества по вопросам, касающимся безопасности информационных систем и сетей,

ДАЕТ УКАЗАНИЕ Комитету ОЭСР по политике в сфере информации, компьютерной техники и связи оказывать содействие в реализации настоящих Директив.

Данная Рекомендация принята взамен прежней Рекомендации Совета по поводу Директив по проблеме безопасности информационных систем от 26 ноября 1992 г. [C(92)188/FINAL].

История принятия документа

Впервые Директивы по проблеме безопасности были приняты в 1992 г., а в 1997 г. они подверглись пересмотру. На этот раз пересмотр Директив был проведен в 2001 г. Рабочей группой по информационной безопасности и неприкосновенности частной жизни (WPISP). Она действовала на основе мандата, полученного от Комитета ОЭСР по политике в сфере информации, компьютерной техники и связи (ИССР), причем после трагедии, произошедшей 11 сентября, работа над документом была ускорена.

Проект Директив был подготовлен Экспертной группой WPISP в ходе заседаний, состоявшихся 10-11 декабря 2001 г. в Вашингтоне (США), 12-13 февраля 2002 г. в Сиднее и 4 и 6 марта 2002 г. в Париже. Заседания WPISP были проведены в Париже 5-6 марта 2002 г., 22-23 апреля 2002 г. и 25-26 июня 2002 г.

Настоящие *“Директивы по проблеме безопасности информационных систем и сетей: формирование культуры обеспечения безопасности”* были приняты в качестве Рекомендации Совета ОЭСР на его 1037-ой Сессии, состоявшейся 25 июля 2002 г.

Оглавление английского оригинала публикации
(без приложений, перечней вставок, таблиц и графиков) :

ДИРЕКТИВЫ ПО ПРОБЛЕМЕ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ И СЕТЕЙ: ФОРМИРОВАНИЕ КУЛЬТУРЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

ПРЕДИСЛОВИЕ

I. ФОРМИРОВАНИЕ КУЛЬТУРЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

II. ЦЕЛИ И ЗАДАЧИ

III. ОСНОВНЫЕ ПРИНЦИПЫ

РЕКОМЕНДАЦИЯ СОВЕТА

ИСТОРИЯ ПРИНЯТИЯ ДОКУМЕНТА

Данный Обзор представляет собой перевод выдержек из публикации ОЭСР, первоначально изданной под следующими английским и французским названиями :

OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security

Lignes directrices de l'OCDE régissant la sécurité des systèmes et réseaux d'information: Vers une culture de la sécurité

© 2002, OECD.

Публикации ОЭСР и Обзоры размещены на сайте

www.oecd.org/bookshop/

Находясь на начальной странице онлайн-магазина, введите в ячейке "Title search" ("Поиск по названию") слово "overview" ("обзор") или наберите название соответствующей книги на английском языке

(На странице, где находится англоязычный оригинал книги, имеется ссылка на соответствующий обзор).

Обзоры подготовлены Отделом прав и переводов Дирекции по общественным делам и связям с общественностью ОЭСР.

Адрес электронной почты : rights@oecd.org / факс: +33 1 45 24 13 91



© OECD, 2003

Репродуцирование данного Обзора разрешается при условии, что будут указаны авторские права ОЭСР и название оригинала публикации.